

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-318894
(P2001-318894A)

(43) 公開日 平成13年11月16日 (2001.11.16)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 5 5
17/60	2 2 2	17/60	2 2 2 5 B 0 8 5
	4 1 4		4 1 4 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B
			6 7 5 D
審査請求 未請求 請求項の数 7 O L (全 12 頁)			

(21) 出願番号 特願2000-381019(P2000-381019)
(22) 出願日 平成12年12月14日 (2000.12.14)
(31) 優先権主張番号 特願2000-58390(P2000-58390)
(32) 優先日 平成12年3月3日 (2000.3.3)
(33) 優先権主張国 日本 (J P)

(71) 出願人 599143058
株式会社エイティン
東京都品川区大井1-23-1
(72) 発明者 藤澤 知徳
東京都品川区大井1-23-1 株式会社エ
ィティング内
(72) 発明者 佐藤 昭治
栃木県黒磯市栄町635
(74) 代理人 100094341
弁理士 石田 政久

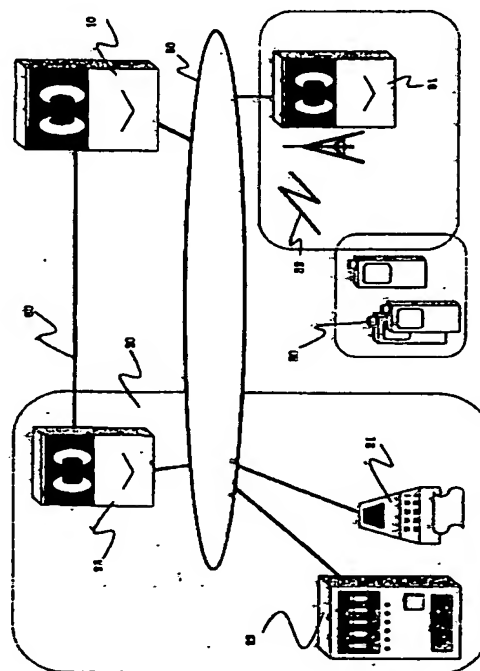
最終頁に続く

(54) 【発明の名称】 個人認証方法

(57) 【要約】

【課題】 携帯端末を使用した、安全で、迅速な個人認証方法を提案する。

【解決手段】 携帯端末30から認証サーバー10に認証を要求すると、認証サーバー10はその携帯端末30に対して認証用の照会記号を発信する。携帯端末30は読取機21などを介した販売管理サーバー23経由で、該照会記号を認証サーバー10に送信し、認証を求める。認証サーバー10は該照会記号を先に生成した照会記号と照合し、その結果と販売管理サーバー23が必要とする個人データを販売管理サーバー23に返信する。



1

【特許請求の範囲】

【請求項 1】 携帯端末の要求に基づき認証サーバーが生成した照会記号を該携帯端末で受け、この照会記号を販売管理サーバーから認証サーバーに戻し、該認証サーバーにおいて前記生成した照会記号と販売管理サーバー経由の照会記号とを照合し、両者が一致したら照会記号に対応する個人情報を該販売管理サーバーに送信することからなる携帯端末を使用した個人認証方法。

【請求項 2】 前記照会記号が前記個人情報と無関係な記号からなる請求項 1 記載の個人認証方法。

【請求項 3】 前記照会記号が当該認証サーバーが過去に生成した照会記号と重複しないものである請求項 1 または請求項 2 記載の個人認証方法。

【請求項 4】 前記携帯端末が受けた照会記号を、前記販売管理サーバーと接続された読取機で読み取る請求項 1～請求項 3 記載の個人認証方法。

【請求項 5】 前記携帯端末が受けた照会記号を、バーコードまたは 2 次元コードとして該携帯端末に表示させ、これを前記読取機で読み取る請求項 1～請求項 4 記載の個人認証方法。

【請求項 6】 前記照会記号が楽音データを含み、これを前記携帯端末の音源で発音させた後、前記読取機で読み取る請求項 1～請求項 4 記載の個人認証方法。

【請求項 7】 前記認証サーバーが照会記号生成後、予め設定した時間に前記生成した照会記号を削除し、前記照合を不能とする請求項 1～請求項 6 記載の個人認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、携帯端末を使用した個人認証方法に関するものである。

【0002】

【従来の技術】 従来、個人の認証方法は、クレジットカードに代表されるように磁気テープを貼付したプラスチックカードによる方法が主流であり、磁気テープに記憶された個人情報をカードリーダーに読み取らせ、それを管理する企業の固有のデータと照合することにより個人を識別している。しかし、カード偽造などの犯罪行為が多発している現状から、近年では偽造し難い IC カード化が進められている。また、オンライン認証の場合は、さらに暗号化技術や暗証番号などを組み合わせることによりセキュリティを強化しているので、カード番号を外部から解読される危険は少ないと言える。更に、携帯端末を使用した個人認証方法としては、利用者が予め信販会社から携帯端末を介して個人認証書の発行を受けておき、代金決済時に携帯端末に記録された前記個人認証書と暗証番号を照合させて個人認証を行う方法が知られている。しかしながら、上記 IC カード化、オンライン認証、携帯端末による個人認証書によるいずれの方法も、「情報の固定化」と「カードライターの存在」という問

2

題点が存在する限り、根本的な問題の解決とはならない。また、今後予想されるサイバービジネス上でのオンライン決済などの問題も解決されていない。

【0003】

【発明が解決しようとする課題】 本発明は、携帯端末を使用した個人認証方法であって、セキュリティの確立されていないネットワーク間では、無意味でかつ非固定的な信号情報を一時的に使用することにより、安全で、迅速な個人認証方法を提案しようとするものである。

【0004】

【課題を解決するための手段】 本発明に係る個人認証方法は、携帯端末の要求に基づき認証サーバーが生成した照会記号を該携帯端末で受け、この照会記号を販売管理サーバーから認証サーバーに戻し、該認証サーバーにおいて前記生成した照会記号と販売管理サーバー経由の照会記号とを照合し、両者が一致したら照会記号に対応する個人情報を該販売管理サーバーに送信することからなる携帯端末を使用した個人認証方法である。前記照会記号は前記個人情報と無関係な記号からなることが好ましい。前記照会記号は当該認証サーバーが過去に生成した照会記号と重複しないものであることが好ましい。前記携帯端末が受けた照会記号を、前記販売管理サーバーと接続された読取機で読み取ることが好ましい。前記携帯端末が受けた照会記号を、バーコードまたは 2 次元コードとして該携帯端末に表示させ、これを前記読取機で読み取ることが好ましい。前記照会記号が楽音データを含み、これを前記携帯端末の音源で発音させた後、前記読取機で読み取ることが好ましい。前記認証サーバーが照会記号生成後、予め設定した時間に前記生成した照会記号を削除し、前記照合を不能とすることが好ましい。

【0005】

【発明の実施の形態】 以下、本発明の好適な実施形態を、図面を参照しながら説明する。図 1 は本発明による個人認証システムの全体説明図であり、同図の点線で囲まれた範囲 20 には、各種商品または各種サービスを提供または販売する現場に配置される読取機 21 や、自動販売機 22 などに内蔵される読取機（図示せず。）と、それらを管理運用する販売管理サーバー 23 がインターネット等のネットワーク 50 により結ばれている状態が示されている。従来、通常のクレジットカード等による代金決済は、この範囲 20 内において行われており、クレジットカードを読取機 21 等に読み取らせ、個人認証を確立させていた。図 1 において、ネットワーク 50 には、携帯端末群 30、30、・・・を運営管理する携帯端末用サーバー 31 が接続され、携帯端末群 30、30、・・・と携帯端末用サーバー 31 とは無線 32 により結ばれている。また、符号 10 は、携帯端末群 30、30、・・・中の各携帯端末 30 に対して個人認証を与える認証サーバーであり、ネットワーク 50 に接続されると共に、販売管理サーバー 23 と専用線 60 で結ば

れている。

【0006】本発明方法では、携帯端末30の所有者が、商品またはサービスの代金支払いの際、または個人の身分証明を行う際、クレジットカードやデビットカード、キャッシュカードまたは各種証明書の代替として、携帯端末30を使用するものであり、その基本原理を図2によって説明する。まず、携帯端末30から認証サーバー10に認証を要求すると（経路201）、認証サーバー10はその携帯端末30に対して認証用の照会記号を発信する（経路202）。携帯端末30は該照会記号を前記読取機21などを介して販売管理サーバー23に送る（経路203）。この読取機21は非接触型の読取機である。販売管理サーバー23は該照会記号を認証サーバー10に送信し、認証を求める（経路204）。認証サーバー10は該照会記号を先に生成した照会記号と照合し、その結果と販売管理サーバー23が必要とする個人情報とを販売管理サーバー23に返信する（経路205）。前記認証用の照会記号は、携帯端末30の要求時に新たに生成され、一時的かつ無意味な記号であり、他の携帯端末30に対しては勿論、当該携帯端末30による次の要求時でも2度と使用されることのない記号である。なお、認証サーバー10と販売管理サーバー23は、物理的に同一のサーバーとなる場合もある。

【0007】再び図1に戻って、前記照会記号の流れを説明する。利用者が商品またはサービス代金の決済手段として、ネットワーク50と結ばれた読取機21や、自動販売機22等を利用して決済を行う場合、最初に個人認証が必要となる。決済を行う利用者は、所有する携帯端末30から認証サーバー10に対して照会記号の送信を要求する。この要求信号は、加入する携帯端末事業者の電波32を経てネットワーク50に接続する為の信号変換サーバーである携帯端末用サーバー31を経由し、認証サーバー10に到達する。認証サーバー10は要求のあった利用者に対する照会記号を作成し、受信した信号経路とは逆の経路を辿って送信する。その照会記号を受け取った携帯端末30は、前記読取機21等に該照会記号を非接触的に読み取らせることにより、照会記号はネットワーク50を通じて、販売管理サーバー23に送信される。

【0008】販売管理サーバー23は該照会記号を照会するために、認証サーバー10に対し照会信号を送信する。この際の実送経路は、ネットワーク50を通じてでも良いが、相互のサーバー間のセキュリティが万全であることが望ましく、専用線60等のような外部にアクセスを許さないような経路が好ましい。認証サーバー10は、その照会信号中の照会記号と先に生成した照会記号とを照合し、その結果と要求事項を販売管理サーバー23に対し返信する。この返信により個人認証が確立され、その後の手続は、信販会社等の固有かつ通常の手続に移行する。

【0009】次に、認証サーバー10に蓄積された個人認証用データファイルの構成を示す図3を用いて、「照会記号」を説明する。図3において、認証サーバー10に備えられたデータ記憶媒体300には、個人認証用データレコード群からなる個人認証用データファイル310が記録されている。各個人認証用データレコード320は、例えば、個々の識別番号である会員NID311とその他の項目312からなり、その中の項目の一つとして「照会記号」321が存在する。即ち、「照会記号」321は、認証サーバー10のデータ記憶媒体300に記憶される個人認証用データレコード群である個人認証用データファイル310において、個人認証用データレコード320中の1フィールドとして存在する1データである。

【0010】ただし、このデータは携帯端末30から要求信号の受信時に初めて生成され、所定の時間内だけ存在し、販売管理サーバー23からの照会信号が一定時間内にない場合には削除される一時的なデータである。また、このデータは固定化されたものではなく、フィールドに生成される毎に相違するデータである。該データは個人認証用データレコードなど、有意の固有データとは別個とし、また固有データを変換もしくは暗号化したものでないことが好ましい。該データの桁数および構成文字は、前記伝達手段の説明からも解るように、人手による入力がかたないため、英数半角文字と一部の半角記号とからなる多数桁、例えば50桁であるとか、場合によっては1000桁が可能であり、天文学的な組み合わせ数となる。

【0011】続いて、認証サーバー10における「照会記号」の生成から削除に至る手順を、図4により説明する。始めに、認証サーバー10は、登録会員の所有する携帯端末30から照会記号の要求を受ける（401）と、登録会員か否かの本人確認を行う。上記本人確認後、認証サーバー10は「照会記号」を生成し（402）、この照会記号は直ちに照会記号生成履歴データに照合され（403）、過去に生成されたかどうかのチェックを受け（404）、重複すると判断された場合は再度照会記号が生成される（405）。これは、過去に生成した照会記号が万一他人に知られていた場合、これと同じ照会記号を使用することによって生じるかもしれない危険性を回避するためである。

【0012】このようにして生成された照会記号が発行され（406）、携帯端末30へ送信される（407）。その後、照会記号は、タイマー等による管理下に置かれ、販売管理サーバー23から照会依頼があったかどうかをチェックし（408）、タイマー等による設定時間内に照会依頼が無いと判断された場合、照会記号は削除される（412）。他方、上記設定時間内に販売管理サーバー23から照会依頼があった場合には、照会記号同士の照合を行った後（410）、要求された個人デ

5

ータを送信し(411)、同時に前記生成した「照会記号」を削除する(412)。

【0013】図5は、認証サーバー10の構成を示すブロック図である。サーバー10は、各種データに対する処理、入出力、送受信を行うために通常備えるべき構成部として、認証サーバー10全体の動作を制御する制御部520と、データ処理を行う処理部530と、各種入出力装置及びネットワーク50等に接続される入出力インターフェース510と、該入出力インターフェース510からデータを受け取る入力部550と、データを出10力する出力部560と、データ処理の際に一時的にデータを記憶する記憶部540と、各種データを受信する受信部570と、各種データを送信する送信部580とを備えている。

【0014】認証サーバー10は、前記通常備えるべき構成部に加えて更に、要求信号または照会信号のIDを判断するID判断部502と、登録IDを蓄積するID蓄積部503と、登録会員番号からその会員情報を検索する登録データ検索部504と、照会記号データなどの会員情報を蓄積する会員情報蓄積部505と、新規の照15会記号データを生成する照会記号生成部506と、新規照会記号データと過去に生成した照会記号データとの重複を照合する照会記号履歴照合部507と、過去に生成した照会記号データを蓄積する照会記号履歴蓄積部508と、照会記号データを携帯端末用の表示形式に変換する表示データ生成部509と、照会信号から要求された個人データを抽出、生成する認証データ生成部511と、新規照会記号データを会員情報の一部として一定時間管理する照会記号タイマー管理部512と、認証データ生成部511が生成した個人データを販売管理サーバ23との間で決められた信号形式に変換する送信信号生成部513と、販売管理サーバ23による照会信号中の照会記号と内部に蓄積してある照会記号とを照合する照会記号照合部514と、を備えている。

【0015】認証サーバー10の作用を説明する。認証サーバー10において、携帯端末30からの照会記号の要求信号は入出力インターフェース510を経由して受信部570へ送られる。処理部530は、制御部520の指示を受け、要求信号が予め登録された信号であるかどうかをID判断部502に問い合わせ、ID判断部502はID蓄積部503のデータと照合し、登録信号であると確認した後、記憶部540へ転送する。転送された要求信号は、制御部520の指示を受けた処理部530によって、該要求信号がどの会員NID311と対応するかを登録データ検索部504に問い合わせられ、登録データ検索部504は会員情報蓄積部505に照合をかけ、該当データを処理部530に知らせる。知らせを受けた処理部530は、照会記号生成部506に対し、20該当データの照会記号フィールドに新規照会記号データを生成するように指示し、生成された新規照会記号デー

6

タを記憶部540に転送する。続いて、処理部530は、その新規照会記号データが過去に生成した照会記号データと重複しないかどうかを、照会記号履歴照合部507に問い合わせる。照会記号履歴照合部507は照会記号履歴蓄積部508に照会し、重複するという知らせを受けた場合は、再度、照会記号生成部506に対し該当データの照会記号フィールドに新規照会記号データを生成するように指示し、これを繰り返す。

【0016】この繰り返しが終了し、次のジョブに進行するのは、重複しないという知らせを処理部530が受け取った場合であり、この時は、該照会記号データを会員情報蓄積部505に蓄積すると同時に、処理部530は表示データ生成部509に指示し、予め決められたデータ形式に変換し記憶部540に送る。予め決められたデータ形式に変換された新規照会記号データは、制御部520の指示を受けた処理部530によって送信部570に転送され、入出力インターフェース510を経由して要求のあった携帯端末30へ送信される。この後、該新規照会記号データは、照会記号タイマー管理部512によって管理され、販売管理サーバ23から一定の時間内に照会信号の受信が無い場合は、照会記号タイマー管理部512によって該新規照会記号データは、自動的25に削除される。

【0017】上記のように、新規照会記号データは表示データ生成部509にてデータ形式が変換されるので、携帯端末30は前記新規照会記号データを種々の形式で受信することができる。例えば、図6に示すように、携帯端末30の液晶モニター600にバーコード601として、2次元コード602として、文字記号データ603として表示させ、これらを各種読取機21で読み取ればよい。バーコード601や2次元コード602は視認30しただけでは意味を探ることができないので最適であるが、文字記号データ603であっても、前記のようにこれらのデータは元々意味を持たない記号であるから、視かれたとしても個人認証用データの安全性は担保されている。携帯端末30が下部接続端子や赤外線通信ポートを備えている場合には、受信した新規照会記号データを、これらの外部接続端子経由で各種販売現場に配置された読取機21等に対して受渡すことができる。勿論、読取機21等が音響カプラーを備えていれば、新規照会記号データを音声データとして受渡すこともできる。新規照会記号データは各種読取機21等から販売管理サーバ23へ送信される。

【0018】販売管理サーバ23は認証サーバー10に対し照会信号を発信し、照会信号は認証サーバー10の入出力インターフェース510を経由して受信部570へと送られる。処理部530では、制御部520の指示を受け、契約関係にある販売管理サーバ23として、該照会信号が予め登録された信号であるかどうかをID判断部502に問い合わせ、ID判断部502はID蓄積部503のデータと照合し、登録信号であると確認した後、記憶部540へ転送する。転送された要求信号は、制御部520の指示を受けた処理部530によって、該要求信号がどの会員NID311と対応するかを登録データ検索部504に問い合わせられ、登録データ検索部504は会員情報蓄積部505に照合をかけ、該当データを処理部530に知らせる。知らせを受けた処理部530は、照会記号生成部506に対し、該当データの照会記号フィールドに新規照会記号データを生成するように指示し、生成された新規照会記号データを記憶部540に転送する。続いて、処理部530は、その新規照会記号データが過去に生成した照会記号データと重複しないかどうかを、照会記号履歴照合部507に問い合わせる。照会記号履歴照合部507は照会記号履歴蓄積部508に照会し、重複するという知らせを受けた場合は、再度、照会記号生成部506に対し該当データの照会記号フィールドに新規照会記号データを生成するように指示し、これを繰り返す。

【0016】この繰り返しが終了し、次のジョブに進行するのは、重複しないという知らせを処理部530が受け取った場合であり、この時は、該照会記号データを会員情報蓄積部505に蓄積すると同時に、処理部530は表示データ生成部509に指示し、予め決められたデータ形式に変換し記憶部540に送る。予め決められたデータ形式に変換された新規照会記号データは、制御部520の指示を受けた処理部530によって送信部570に転送され、入出力インターフェース510を経由して要求のあった携帯端末30へ送信される。この後、該新規照会記号データは、照会記号タイマー管理部512によって管理され、販売管理サーバ23から一定の時間内に照会信号の受信が無い場合は、照会記号タイマー管理部512によって該新規照会記号データは、自動的に削除される。

【0017】上記のように、新規照会記号データは表示データ生成部509にてデータ形式が変換されるので、携帯端末30は前記新規照会記号データを種々の形式で受信することができる。例えば、図6に示すように、携帯端末30の液晶モニター600にバーコード601として、2次元コード602として、文字記号データ603として表示させ、これらを各種読取機21で読み取ればよい。バーコード601や2次元コード602は視認しただけでは意味を探ることができないので最適であるが、文字記号データ603であっても、前記のようにこれらのデータは元々意味を持たない記号であるから、視かれたとしても個人認証用データの安全性は担保されている。携帯端末30が下部接続端子や赤外線通信ポートを備えている場合には、受信した新規照会記号データを、これらの外部接続端子経由で各種販売現場に配置された読取機21等に対して受渡すことができる。勿論、読取機21等が音響カプラーを備えていれば、新規照会記号データを音声データとして受渡すこともできる。新規照会記号データは各種読取機21等から販売管理サーバ23へ送信される。

【0018】販売管理サーバ23は認証サーバー10に対し照会信号を発信し、照会信号は認証サーバー10の入出力インターフェース510を経由して受信部570へと送られる。処理部530では、制御部520の指示を受け、契約関係にある販売管理サーバ23として、該照会信号が予め登録された信号であるかどうかをID判断部502に問い合わせ、ID判断部502はID蓄積部503のデータと照合し、登録信号であると確認した後、記憶部540へ転送する。転送された要求信号は、制御部520の指示を受けた処理部530によって、該要求信号がどの会員NID311と対応するかを登録データ検索部504に問い合わせられ、登録データ検索部504は会員情報蓄積部505に照合をかけ、該当データを処理部530に知らせる。知らせを受けた処理部530は、照会記号生成部506に対し、該当データの照会記号フィールドに新規照会記号データを生成するように指示し、生成された新規照会記号データを記憶部540に転送する。続いて、処理部530は、その新規照会記号データが過去に生成した照会記号データと重複しないかどうかを、照会記号履歴照合部507に問い合わせる。照会記号履歴照合部507は照会記号履歴蓄積部508に照会し、重複するという知らせを受けた場合は、再度、照会記号生成部506に対し該当データの照会記号フィールドに新規照会記号データを生成するように指示し、これを繰り返す。

7

D蓄積部503のデータと照合し登録された信号であることを確認後、記憶部540へと転送する。次に、処理部530は、転送された照会信号の照合を照会記号照合部514に指示する。照会記号照合部514は、記憶部540の照会信号から照会記号を抽出し、照会記号の蓄積された会員情報蓄積部505に対し照合をかけ、照合の結果一致するものがあった場合、その会員NID311を処理部530に返す。

【0019】会員NID311を受けた処理部530は、認証データ生成部511に指示し、前記転送された照会信号からの要求に必要な個人データを会員情報蓄積部505より抽出、生成する。この個人データは、制御部520の指示を受けた処理部530によって、記憶部540に転送される。この記憶部540内の個人データは、制御部520の指示を受けた処理部530の指示により、送信信号生成部513によって、予め販売管理サーバー23との間で決められた信号形式、例えば、公開鍵暗号方式や共通鍵暗号方式等に変換され、送信部580に転送され、入出力インターフェース510を経由して要求のあった販売管理サーバー23に伝信される。このように本実施形態では、インターネット等の無防備なネットワーク上では、悪意の傍受があることを前提とし、その対策として、一時的に発信した無意味な信号のみを利用し、意味のある信号の流通を行わないと共に、よりセキュリティの高いシステム間においてだけ意味のある信号を利用するものである。

【0020】次に、本発明の他の好適な実施形態を説明する。上述した無意味でかつ非固定的な「照会記号」は一回毎に使い捨てる必要があり、本発明の実用化には膨大な数の照会記号が要求される。ところが、前記「バーコード利用」の場合、13桁(JANコードの場合)で表現される数値の組合わせである為、JANコードのルールは別としても10の13乗分の組合わせ数でしかない。また、「二次元コード」も、その組合わせ数は、二次元コードの理論上バーコードの数百倍でしかない。更に「英数字の組合わせ画面」に於いては、携帯端末の画面の表示能力によるが、一度に表示可能な桁数はせいぜい100桁が最大と考えられ、その組合わせ数は36の100乗である。次に詳述する実施形態は、この「組合わせ数」を飛躍的に増大させることを企図するものであり、携帯電話等に装着される音源を利用し、楽音信号を照会記号として利用するものである。本実施形態では、認証サーバー10に楽音信号発生部70を備え、かつ、読取機21として楽音認識部80を備えることを特徴とする。

【0021】図7は、楽音信号発生部70のブロック図であり、楽音信号発生部70は、少なくともワンフレーズ分の楽音信号を自動生成させる楽音信号生成部71と、過去に生成した楽音信号を蓄積しておく楽音信号蓄積部72と、自動生成された楽音信号中のデータを照会

8

記号として利用する部署、即ち、認証サーバー10の照会記号照合部514に転送する楽音信号転送部73と、前記自動生成された楽音信号を携帯端末30に送信する楽音信号送信部74とから構成されている。

【0022】図7において、携帯端末30の要求に基づき処理部530の指示を受けた楽音信号生成部71は、予め設定されたフレーズ数内で、楽音データを含む楽音信号をランダムかつ自動的に生成する。当該楽音信号は、音の高低と長短に関する楽音データのみならず、音色、音調などに関する楽音データを含むものであっても良い。前記楽音信号は、楽音信号蓄積部72に蓄積された楽音信号と照合され、新生のものと判断された場合には、楽音信号転送部73と楽音信号送信部74の2方向に転送される。即ち、前記認証サーバー10の作用の項で説明したのと同様に、楽音信号は楽音信号転送部73から照会記号照合部514に転送されると共に、楽音信号送信部74では、照会要求者の携帯端末30において音源信号を発音させる為に、楽音信号を携帯端末所定の形式に変換して送信する。

【0023】図8は、読取機21における楽音認識部80を中心とするブロック図であり、同図には携帯端末30の音源で発音された楽音を電気信号として入力するマイク81と、マイク81に入力されたアナログ信号をデジタル変換するA/D変換部82と、変換されたデジタル信号を元の楽音信号として認識する楽音認識部80と、認識された楽音信号を販売管理サーバー23へ送信する送信コントロール部83とが図示されている。前記楽音認識部80は、デジタル信号を元の楽音信号として認識する際、デジタル信号を作業用に一時保管するメモリ部85と、メモリ部85に記録された楽音パターンと照合すべき標準パターンを記憶しておく楽音認識辞書部86と、前記デジタル信号の照合、判断を行う楽音認識管理部87とから構成される。

【0024】図8において、マイク81から入力されたアナログ信号は、A/D変換部82でデジタル信号に変換され、楽音認識部80へ送られる。当該デジタル信号は、楽音認識管理部87の指示によりメモリ部85に一時保管されると共に、楽音認識管理部87によってデジタル信号中の楽音データ(音の高低、長短など)が解析され、解析された楽音データと楽音認識辞書部86に蓄積された標準パターンとが照合、判断される。蓄積すべき標準パターン数を減量化するためには、前記楽音データの解析を音符単位として個別に行うことが好ましい。楽音認識部80で楽音認識された楽音信号は送信コントロール部83を経て、前記認証サーバー10の作用の項で説明したのと同様に、販売管理サーバー23へ送信される。

【0025】

【発明の効果】請求項1記載の発明によれば、携帯端末を利用して安全で、迅速な個人認証を確立することがで

10

20

30

40

50

9

きる。従って、偽造され易いクレジットカードやデビットカード、キャッシュカードまたは各種証明書などの固定的なデータまたはそれらを暗号化したデータの盗難・解読事故を防ぐことが可能であるばかりでなく、今後利用が見込まれるサイバービジネス上の決済手段としても極めて有効である。請求項2または請求項3記載の発明によれば、より一層、セキュリティを向上させることができる。請求項4または請求項5記載の発明によれば、手軽で迅速な個人認証が実現可能となると共に、携帯端末は読取機と非接触状態でデータ移動することができるので、携帯端末を破損といったトラブルが生じる虞がない。請求項6記載の発明によれば、携帯端末に装着される音源を利用し、音の高低と長短または音色、音調等に関する楽音データを利用することにより、「照会記号」を略無尽蔵とすることができるものである。請求項7記載の発明によれば、より一層、個人認証に対する信頼性を向上させることができる。

【図面の簡単な説明】

【図1】本発明による個人認証システムの全体説明図である。

【図2】本発明方法の基本原理を示す説明図である。

10

*【図3】認証サーバー10に蓄積された個人認証用データファイルの構成図である。

【図4】認証サーバー10における「照会記号」の生成から削除に至る手順を示すフロー図である。

【図5】認証サーバー10の構成を示すブロック図である。

【図6】照会記号データの携帯端末モニターにおける表示例である。

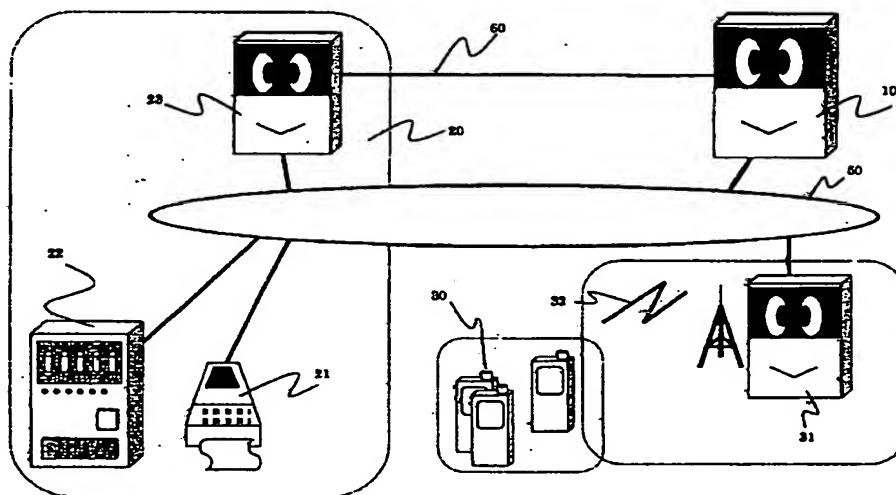
10 【図7】認証サーバー10における楽音信号発生部70の構成を示すブロック図である。

【図8】読取機21における楽音認識部80を中心とする構成を示すブロック図である。

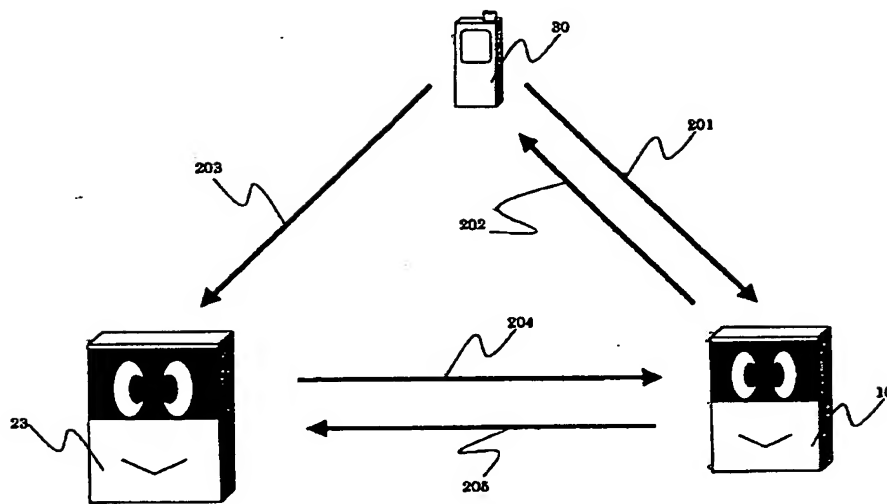
【符号の説明】

- 10 認証サーバー
- 21 読取機
- 23 販売管理サーバー
- 30 携帯端末
- 50 ネットワーク
- 60 専用線
- 70 楽音信号発生部
- 80 楽音認識部

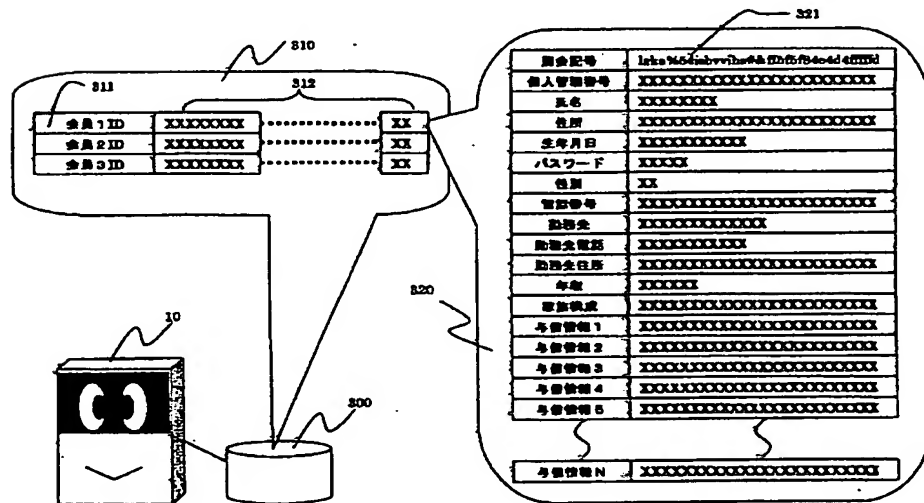
【図1】



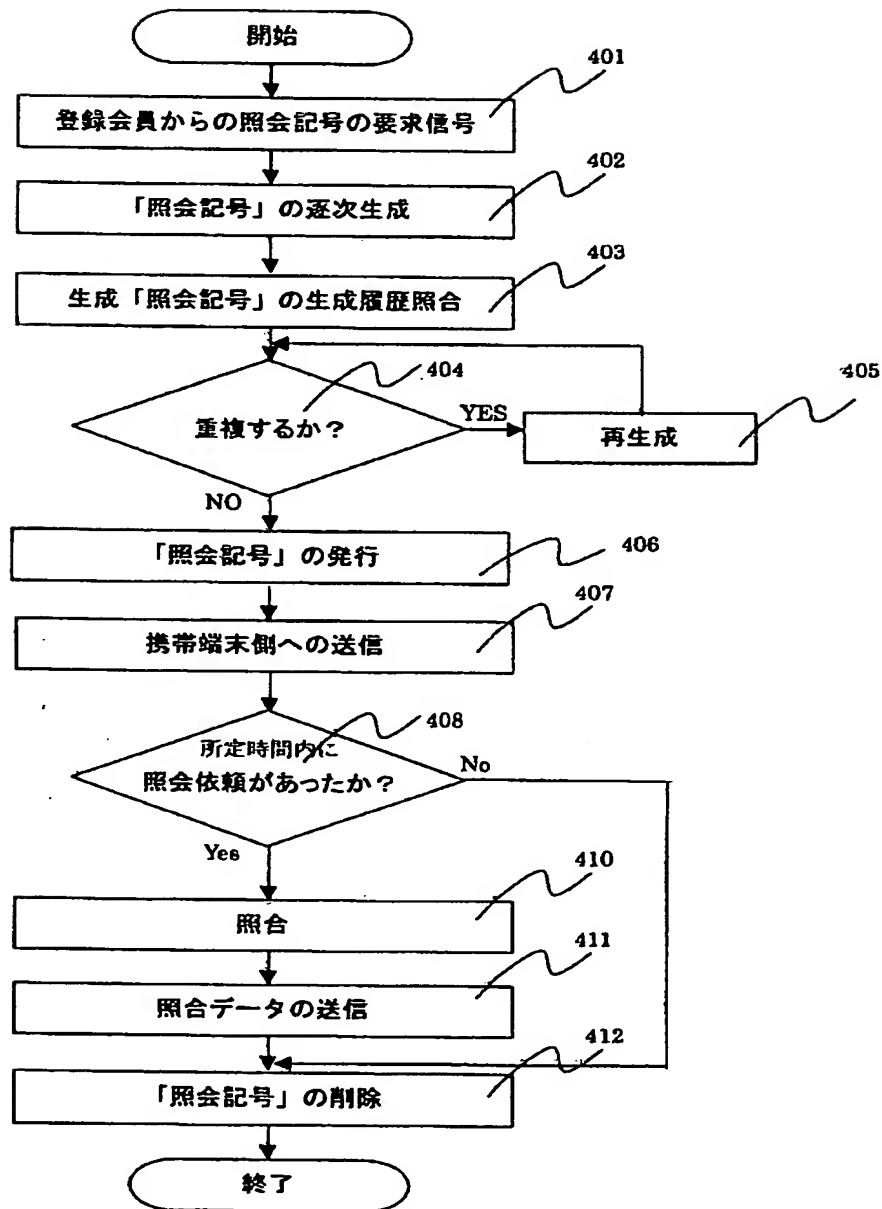
【図2】



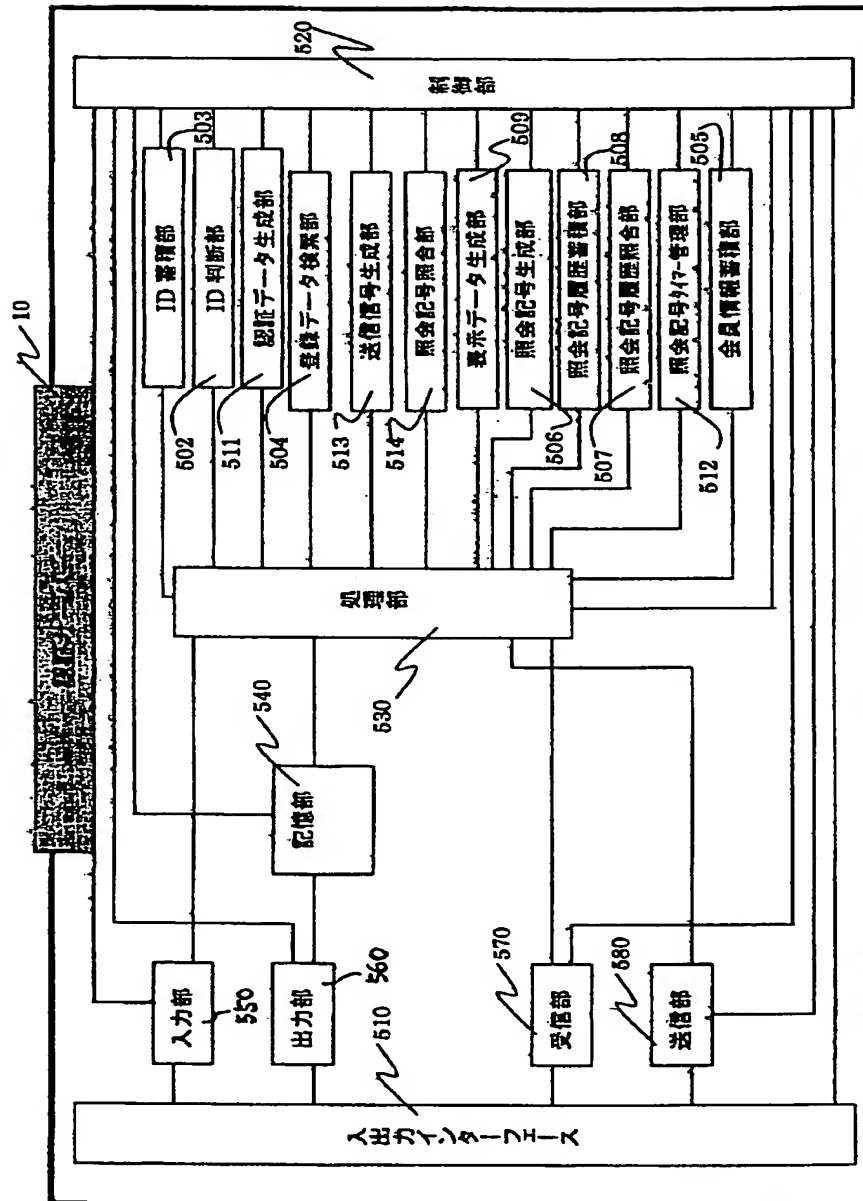
【図3】



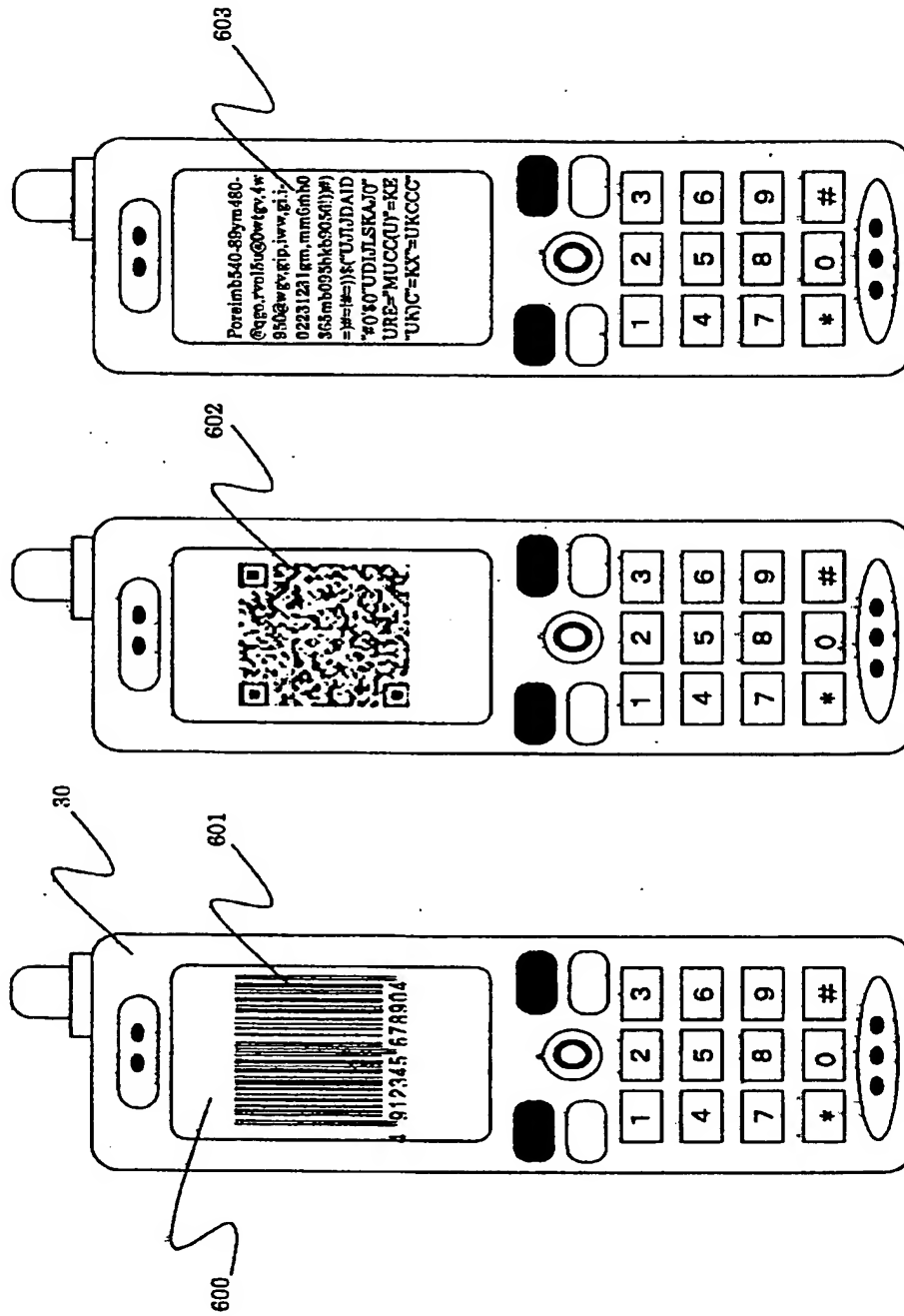
【図4】



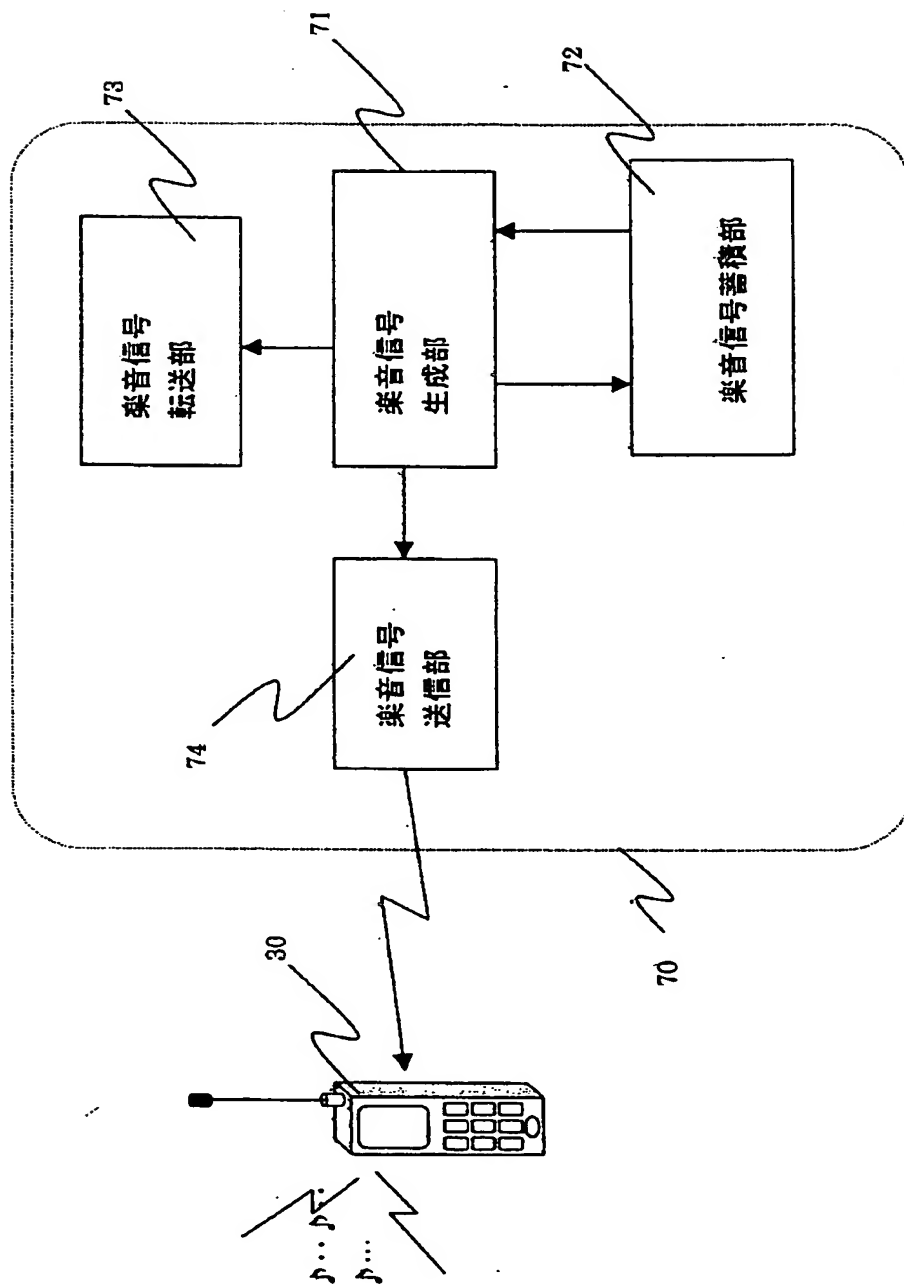
【図5】



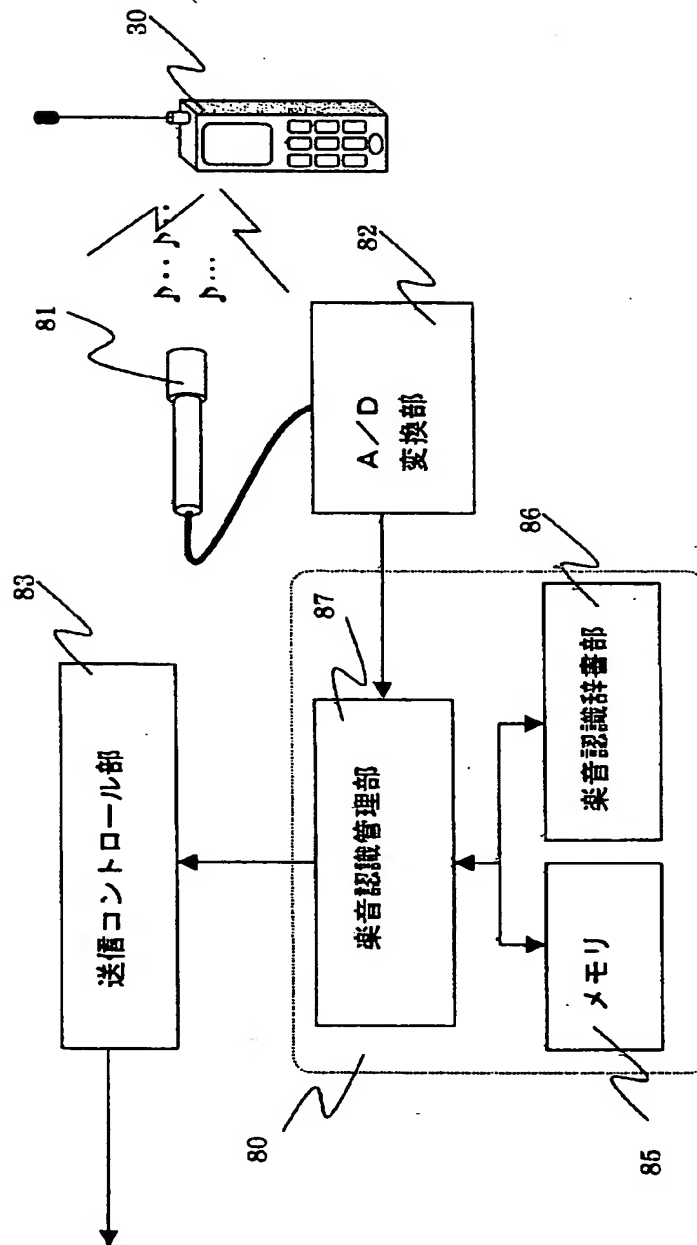
【図6】



【図7】



【図8】



フロントページの続き

Fターム(参考) 5B055 BB12 HA01 HA08
 5B085 AA01 AE01 AE23 BC02 BE01
 BE07
 5J104 AA07 KA02 KA04 KA21 MA02
 NA36 NA38